CONTINUATION PAGES OF SEARCH WARRANT

…hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain mobile telephone that was seized during a search warrant by officers of the Lycoming Regional Police Department (LRPD) during the investigation of an incident where counterfeit Federal Reserve Notes (FRNs) were passed/uttered in the Williamsport, PA area. The phone is an Apple iPhone in a green colored case with a cracked screen. The items to be seized are further described in Attachment A.

2. I am a Special Agent with the United States Secret Service (USSS), Harrisburg Resident Agency, and have been a Special Agent for 17 years. As a Special Agent with the USSS, I am an "investigative or law enforcement officer" within the meaning of Title 18 United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations and to make arrests for offenses enumerated in Titles 18 of the United States Code, among other things. I am thoroughly familiar with the information contained in this

affidavit, based upon the investigation that I have conducted with other experienced law enforcement officers, my communications with witnesses, and my review of relevant documents and materials.

3. As a Special Agent with the USSS, I have participated in investigations involving wire fraud, bank fraud, complex financial crimes, and counterfeiting. During these investigations, I have conducted or participated in the execution of search warrants, witness interviews and document analysis in furtherance of these investigations. The review of digital evidence has yielded substantial evidence, including financial records, transactional logs and other relevant records. Through my training, education and experience, I have become familiar with the manner in which counterfeiting offenses are committed, including the ways in which electronic communications, made through cellular telephones, further those offenses.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title

18, U.S.C. Section 472 (Passing/Uttering Counterfeit Federal Reserve Notes) and Title 18, U.S.C Section 371 (Conspiracy to Pass/Utter Counterfeit Federal Reserve Notes), have been committed by Ezra Figueroa and others, there is probable cause to believe that Figueroa and others conspired to pass/utter counterfeit FRNs at several businesses in the Middle District of Pennsylvania and elsewhere.

6. An Apple iPhone (TARGET PHONE), in a green colored case with a cracked screen, that was seized during a search warrant by the LRPD on September 19, 2023 and is currently in the possession of United States Secret Service, is the TARGET PHONE of this search warrant. There is probable cause to search the information described in Attachment A for evidence, instrumentalities, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant under Rule 41 of the Federal Rules of Criminal Procedure because the requested warrant would permit the search and seizure of "property located within the district," Fed. R. Crim. P. 41(b)(1), and because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C.

§§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . in or for a district . . . in which the wire or electronic communications, records, or other information are stored." 18 U.S.C. § 2711(3)(A)(ii).

RELEVANT STATUTES AND REGULATIONS

A. Offenses

8. Federal law prohibits uttering counterfeit obligations or securities: "Whoever, with the intent to defraud, passes, utters, publishes, or sells, or attempts to pass, utter, publish, or sell, or with like intent brings into the United States or keeps in possession or conceals any falsely made, forged, counterfeited, or altered obligation or other security of the United States, shall be fined under this title or imprisoned not more than 20 years, or both." 18 U.S.C. § 472.

PROBABLE CAUSE

9. In June of 2023, the USSS began investigating a series of incidents where individuals passed counterfeit FRNs in order to make purchases and upload funds to accounts. The scheme involved the individuals using a mobile telephone to produce a scannable code to facilitate the transaction. During the investigation Rovaney Doe,

Antonius Gayflorsee, Moses Yallah, Elhadj Saysay, and Ezra Figueroa, were identified through various means as the individuals engaged in the scheme, as well as other individuals that have yet to be identified. The individuals were observed in video surveillance using mobile telephones to scan codes at the time of the transactions, communicate, as well as using the "tap to pay" function on the devices.

10. The investigation includes conduct from the Spring of 2023 to the Fall of 2023, with approximately $8,900 in counterfeit FRNs passed in the Middle District of Pennsylvania and approximately $17,450 passed in other parts of Pennsylvania and Virginia. There were approximately 28 incidents during that time frame, involving 25 law enforcement agencies.

11. On September 18, 2023, the LRPD was dispatched to a Dollar General for an individual attempting to pass a counterfeit $50 FRN. The responding officer was able to speak with witnesses, review surveillance footage from the incident, and obtain a description of the suspect and vehicle.

12. The responding officer located a vehicle that matched the one from the initial Dollar General in the parking lot of a Family Dollar nearby. The vehicle left the parking lot and a traffic stop was initiated.

13. The officer found that the driver of the vehicle, Ezra Figueroa, was the suspect from the incident at the Dollar General. Figueroa was charged for Forgery and Theft by Deception. The vehicle was impounded and secured pending the application for a search warrant.

14. Rovaney Doe, Elijah Zeyon, and Carl S. Johnson, Jr were occupants of the vehicle. Doe provided officers with an alias of Jason Tindal-Ferguson.

15. On September 19, 2023, a search warrant for the vehicle and its contents was obtained. During the search officers located an Apple iPhone in a green colored case with a cracked screen on the rear seat of the vehicle. Officers also recovered $10,670 in counterfeit FRNs from the vehicle. Some of the counterfeit FRNs were found hidden in a zippered compartments behind the driver's and front passenger's seat. They also found counterfeit or forged checks, a Pennsylvania Driver's License belonging to Justin S. Hamilton, and a Citizens Bank card in the name of Patricia Sluwar, Rovaney Doe's mother.

16. On September 22, 2023, officers went back to the Family Dollar the vehicle was seen parked in and spoke with employees. They determined Ezra Figueroa passed $600 in counterfeit FRNs at the business. Figueroa initially made a purchase with a counterfeit $100 FRN and was given $79.70 in change. The items purchased were located in the vehicle during the search warrant. He then used $500 in counterfeit FRNs to upload funds to "Cash App" account. Family Dollar employees told officers that Figueroa was used a cellular phone with "light green cover and cracked screen" as a means of showing a bar code to upload the funds.

17. As set forth above, there is furthermore probable cause to believe that the TARGET PHONE will contain evidence of Figueroa's passing/uttering

TECHNICAL TERMS

18. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *Wireless telephone*: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These

telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. *Digital camera*: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be

retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. *Portable media player*: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. *GPS*: A GPS navigation device uses the Global Positioning System to display its current location. It often contains

records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. *PDA*: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually

include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. *Tablet*: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example,

permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. *Pager*: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

h. *IP Address*: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

i. *Internet*: The Internet is a global network of computers and other electronic devices that communicate with each other. Due

to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

19. Based on my training, experience, and research, I know that the TARGET PHONE has capabilities that allow it to serve as wireless telephones, digital cameras, portable media players, GPS navigation devices, PDAs, tablets, and pagers, with associated IP addresses and access to the internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

20. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

21. Even if a person obtains a new mobile phone, it is common for records stored on a prior mobile phone to be transferred to the new phone. For example, electronic communications such as emails and text

messages are regularly transferred so that they may be accessed from the new phone. Likewise, data stored in mobile-phone applications, such as contacts, photos, videos, saved downloads, and other content, is typically transferred so that the mobile phone user may continue to use the same applications and data on the new mobile phone. In short, records from years before are often still accessible due to the ways in which data are transferred and stored over time. Where such records have been deleted, there are sometimes ways to see that such deletions have occurred.

22. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the TARGET PHONE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the TARGET PHONE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

23. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

24. *Manner of execution.* This warrant seeks permission to examine devices that will be obtained from the holder of the device. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

25. Your affiant knows that individuals who associate with each other in criminal activities often communicate by text message, email, voice mail, etc., and often take photos of themselves using devices like

the TARGET PHONE. It is believed that such evidence would constitute evidence of guilt of Figueroa and a criminal association involving Rovaney Doe, Antonius Gayflorsee, Moses Yallah, and Elhadj Saysay. The TARGET PHONE itself was used in facilitating the passing/uttering of counterfeit FRNs. It is evidence of a crime and an instrumentality used in the commission of a crime.

26. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c). I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the TARGET PHONE described in Attachment A to seek the items described in Attachment B. If necessary to effectuate the search of the TARGET PHONE described in Attachment A and seizure of the items described in Attachment B.